VIRUS RESPONSE PROCESS NOTES

(1) The server administrator who discovers a potential infection is responsible for immediately investigating the situation or immediately turning that responsibility over to a more appropriate person with confirmation that immediate action will be taken.

(2) Anything out of the ordinary should be investigated.

(3) Use the installed virus protection product. If viruses are detected but not eradicated, or are suspected but not detected, then use the additional tools available from the Software Library. Where an installed product runs automatically, start by reviewing the report.

(4) If a group area on a server is affected, open a "P1E" ticket for each group area, identify the users affected, and have the Service Center page the PR Team so that the appropriate desktop(s) can be checked. The SOC should "own" the ticket(s).

(5) If a user's home area on a server is affected, open a "P1" ticket for each affected user and have the PR Team paged so that the appropriate desktop(s) can be checked. The SOC should "own" the ticket(s).

(6) If the system area of a server is affected, open a "P1" ticket for the server. The SOC should "own" the ticket.

(7) Once the server issue(s) have been worked and resolved, the server ticket(s) should be closed. If assistance is required, it should be requested from the Boeing IT Security Team. If assistance is requested, the SOC continues to "own" the ticket.

(8) When the Service Center receives a virus call, the first step should be to confirm the user's suspicion that his/her desktop is or was infected.

(9) In the case of an actual infection, the Service Center should review with the user their responsibilities as detailed in the "User Responsibilities" column (front, right).\

(10) Rather than immediately paging the PR Team, the Service Center should offer to assist and educate the user regarding the use of the installed virus protection product.

(11) If the user issue(s) have been worked and resolved, then the user ticket may be closed. If not, then the user should be reminded of the necessity to place a note on the monitor indicating a suspected virus and to wait for the PR Team to respond. The Service Center should then turn the user ticket over to the PR Team and page it out (for response in less than one hour).

(12) If a user suspects that their Mac or PC desktop is infected, they must immediately cease processing, leave the Mac/PC powered up, leave any diskettes mounted and notify the Service Center.

(13) When a user ticket is turned to the PR Team, the appropriate member of the Team should respond within one hour (this is a contract metric).

(14) The PR Team should use the installed virus protection product and other appropriate tools as necessary to resolve the user issue(s).

(15) If the user issue(s) have been worked and resolved, then the user ticket should be closed. If assistance is required, it should be requested from the Boeing IT Security Team. If assistance is requested, the PR Team continues to "own" the ticket.